(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
20. September 2001 (20.09.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/69548 A1

(51) Internationale Patentklassifikation[7]: G07F 7/08, 7/10

(21) Internationales Aktenzeichen: PCT/CH00/00149

(22) Internationales Anmeldedatum:
15. März 2000 (15.03.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **SWISSCOM MOBILE AG** [CH/CH]; Schwarztorstrasse 61, CH-3050 Bern (CH).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: **LAUPER, Eric** [CH/CH]; Schützenweg 12, CH-3014 Bern (CH). **CANTINI, Renato** [CH/CH]; 35, route du Moulin, CH-1782 Belfaux (CH).

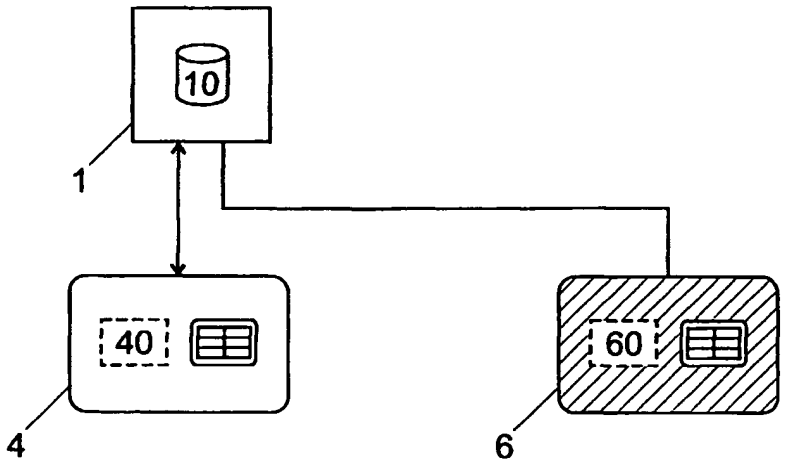
(74) Anwalt: **SAAM, Christophe**; Patents & Technology Surveys SA, (AG, Ltd), Faubourg du Lac 2, P.O. Box 1448, CH-2001 Neuchatel (CH).

(81) Bestimmungsstaaten *(national)*: AE, AL, AM, AT, AT (Gebrauchsmuster), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, CZ (Gebrauchsmuster), DE, DE (Gebrauchsmuster), DK, DK (Gebrauchsmuster), DM, DZ, EE, EE (Gebrauchsmuster), ES, FI, FI (Gebrauchsmuster), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Gebrauchsmuster), SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR DISTRIBUTING PARAMETERS IN OFFLINE CHIPCARD TERMINALS AND APPROPRIATE CHIPCARD TERMINALS AND USER CHIPCARDS

(54) Bezeichnung: VERFAHREN ZUR VERBREITUNG VON PARAMETERN IN OFFLINE CHIPKARTEN-TERMINALS, SOWIE DAZU GEEIGNETE CHIPKARTEN-TERMINALS UND BENUTZERCHIPKARTEN



(57) Abstract: The invention concerns a method for updating transient parameters (50), especially lists of blocked user chipcards, in offline chipcard terminals (5), wherein the above-mentioned parameters are updated with the user chipcards (4) used in said offline chipcard terminal (5). One advantage is that the offline terminals must not be inspected manually.

(57) Zusammenfassung: Verfahren zur Aktualisierung von vergänglichen Parametern (50), insbesondere Listen von gesperrten Benutzerchipkarten, in Offline-Chipkarten-Terminals (5), in welchen die benannten Parameter mit den im benannten Offline-Chipkarten-Terminal (5) verwendeten Benutzerchipkarten (4) aktualisiert werden. Vorteil: die Offline-Terminals müssen nicht manuell inspiziert werden.

WO 01/69548 A1

(84) **Bestimmungsstaaten** *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:
— *mit internationalem Recherchenbericht*

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Verfahren zur Verbreitung von Parametern in Offline Chipkarten-Terminals, sowie dazu geeignete Chipkarten-Terminals und Benutzerchipkarten.

Die vorliegende Erfindung betrifft ein Verfahren zur Verbreitung von Parametern in Offline Chipkarten-Terminals, sowie dazu geeignete Chipkarten-Terminals und Benutzerchipkarten.

Chipkarten-Terminals werden immer häufiger als Identifizierungsmittel für verschiedene Systeme und als tragbarer Datenspeicher mit Datenverarbeitungsfähigkeiten verwendet. Es ist unter anderem bekannt, dass man Chipkarten als elektronische Geldbörse zum Bezahlen in verschiedenen Verkaufsstellen verwenden kann. Vorstellbare Anwendungen für Chipkarten als elektronische Geldbörse umfassen unter anderem Lebensmitteleinzelhandel, Kaufhäuser, Parkraumbewirtschaftung, öffentliche Verkehrsmittel, Personenverkehr (Taxi), Tankstellen, Hotels und Gaststätten, Kantinen und Mensen, Getränke- und Verpflegungsautomaten, Straßenbenutzungsgebühren, Eintrittskartenverkauf, Zutrittskontrollgeräte, öffentliche Telekommunikationsdienstleistungen, Internet, Online-Dienste, Pay-TV, usw.. Ausserdem ist auch bekannt, dass man Chipkarten als reines Benutzeridentifizierungsmittel verwenden kann, beispielsweise in Mobilfunktelefonen (SIM-Karten) oder als Zutritts-Karte.

Diese verschiedenen Benutzungsstellen verwenden Chipkarten-Terminals, die die Benutzerchipkarte mit Strom versorgen und die eine datentechnische Verbindung mit der Karte herstellen können, beispielsweise um die Identifizierung in der Karte zu lesen oder um elektronisches Geld zu überweisen. Solche Terminals können entweder an bestehende Systeme (beispielsweise Kassensysteme) angeschlossen oder als 'stand alone'-Gerät gehandhabt werden.

Um die Identität der Benutzer zu überprüfen, wird oft vom Benutzer verlangt, dass er ein Geheimnis eingibt, beispielsweise eine PIN oder biometrische Parameter. Um dieses zu überprüfen, werden Terminals oft Online mit einer Zentrale verbunden, beispielsweise über ein privates oder

öffentliches Telekommunikationsnetz. Diese Online Verbindung wird auch eingesetzt, um elektronische Geldeinheiten zu überweisen und um vergängliche (für mindestens eine gewisse Zeitdauer gültige) Terminalparameter zu aktualisieren, beispielsweise um Listen von gesperrten Karten in Terminals so schnell wie möglich zu verteilen.

Eine solche permanente Verbindung zwischen Terminal und Zentrale ist jedoch teuer. Soll die Benutzerchipkarte auch zur Bezahlung von kleinen Beträgen verwendet werden, beispielsweise am Kiosk, für Buskarten, usw., kann der Preis für die Verbindung in gewissen Fällen einem beträchtlichen Teil des Transaktionswert entsprechen. Ausserdem ist die Verbindung eines Terminals mit einem Telekommunikationsnetz oft technisch nicht oder nur mit viel Aufwand machbar, beispielsweise wenn der Terminal entfernt von jedem verfügbaren telefonischen Anschlusspunkt installiert werden muss.

Um diese Verbindungskosten zu vermeiden, hat man auch sogenannte Offline-Terminals entwickelt, die autark arbeiten können, ohne mit einer übergeordneten Zentrale verbunden zu sein. Typische Offline-Chipkartenterminals werden beispielsweise bei Händlern verwendet, wenn die durchschnittlich bezahlten Beträge in der gleichen Grössenordnung wie die Verbindungskosten sind.

Es sind ausserdem sogenannte Hybrid-Terminals bekannt, die mit einem Telekommunikationsnetz nur ab und zu verbunden sind (beispielsweise einmal täglich), um alle Transaktionen des Tages auf einmal an die Zentrale zu senden.

Ein Problem mit Offline- und Hybrid-Terminals ist die Aktualisierung von vergänglichen Parametern. Jeder Terminal verwendet in der Regel eine Reihe von nicht dauerhaften und nicht mit einer spezifischen Transaktion verbundenen Parameter, die ab und zu (beispielsweise mehrmals in der Woche) aktualisiert werden müssen. Solche Parameter umfassen unter anderem Listen von gesperrten Benutzerchipkarten (beispielsweise

ungültigen, nicht mehr gültigen oder fraudulent eingesetzten Benutzerchipkarten) sowie Transaktionstarife.

Im Falle von Chipkarten-Terminals, die auch für Geldtransaktionen mit Geldkarten verwendet werden, umfassen diese vergänglichen Parameter auch die Liste der durchgeführten Transaktionen, die in die Zentrale übertragen werden muss, sowie den Inhalt der elektronischen Geldkonten, der überwiesen werden muss.

Solche Parameter werden in der Regel manuell aktualisiert, indem ein Angestellter alle Terminals verifiziert und die vergänglichen Parameter aus einem oder in ein tragbares Gerät kopiert, das dann mit der Zentrale verbunden wird. Im Falle eines tragbaren Chipkarten-Terminals kann er auch selbst an einen Anschlusspunkt der Zentrale gebracht werden, wie in WO9517738 beschrieben. Dieser manuelle Aktualisierungsvorgang ist jedoch aufwendig, vor allem wenn viele breit verstreute Terminals inspiziert werden müssen.

Ausserdem müssen die Chipkarten-Terminals Eingabemittel (beispielsweise eine Tastatur, eine Schnittstelle zum Aktualisierungsgerät, eventuell eine Anzeige) beinhalten, die vom Angestellten bedient werden, um die Parameter zu aktualisieren. Solche Eingabemittel verteuern den Terminal und verlangen ein grösseres Gehäuse.

Es ist ein Ziel der vorliegenden Erfindung, ein neues Verfahren anzubieten, mit welchem die benannten Parameter mit weniger Aufwand aktualisiert werden können.

Gemäss der vorliegenden Erfindung werden diese Ziele insbesondere durch die Merkmale der unabhängigen Ansprüche erreicht. Weitere vorteilhafte Ausführungsformen gehen ausserdem aus den abhängigen Ansprüchen und der Beschreibung hervor.

Insbesondere werden diese Ziele durch ein Verfahren erreicht, in welchem vergängliche Parameter in Offline Chipkarten-Terminals mit den

im Chipkarten-Terminal verwendeten Benutzerchipkarten aktualisiert werden.

Insbesondere werden vergängliche Parameter, beispielsweise Listen von gesperrten Benutzerchipkarten, Tarife, usw. in Benutzerchipkarten, vorzugsweise chiffriert und/oder in einen gesicherten, dem Benutzer der Chipkarte nicht zugänglichen Speicherbereich der Benutzerchipkarte kopiert und über diese Benutzerchipkarten von Terminal zu Terminal übertragen.

Dieses Verfahren ist insbesondere in Systemen geeignet, in welchen dieselben Benutzerchipkarten sowohl in Offline als auch in Online Chipkarten-Terminals verwendet werden. Dies ist insbesondere der Fall in Hybrid-Systemen, in welchen nicht alle Terminals Online verbunden sind, aber auch für Systeme mit Benutzerchipkarten, die für verschiedene Anwendungen verwendet werden, beispielsweise für SIM-Karten, die auch als Wertkarten für Offline Terminals eingesetzt werden können.

Ein Vorteil der vorliegenden Erfindung ist, dass jede Benutzerchipkarte vor allem Parameter die andere Benutzerchipkarte betreffen enthält, beispielsweise Listen von anderen gesperrten Benutzerchipkarten. Der Karten-Inhaber ist nicht in der Lage, die Parameter zu ändern und wird übrigens kaum Gründe finden, zu versuchen, die Karte zu fälschen und Parameter für andere Karten zu ändern.

Ein anderer Vorteil ist es, dass keine zusätzlichen Chipkarten notwendig sind, um die benannten vergänglichen Parameter in Offline-Terminals zu aktualisieren. Es werden nur die Benutzerchipkarten benötigt, die auch für normale Transaktionen mit Online- und/oder Offline-Terminals verwendet werden. Für den Benutzer ist der Vorgang völlig transparent und es wird von ihm nicht verlangt, dass er andere Schritte oder Aktionen als für normale Transaktionen mit den Terminals unternimmt.

Im Folgenden werden anhand der beigefügten Zeichnungen bevorzugte Ausführungsbeispiele der Erfindung näher beschrieben:

Die Figur 1 zeigt schematisch ein System mit einer Zentrale, einer Vielzahl von Online-Chipkarten-Terminals und einer Benutzerchipkarte gemäss der Erfindung.

Die Figur 2 zeigt schematisch ein System mit einem Offline-Chipkarten-Terminal, einer erfindungsgemässen Benutzerchipkarte und einer gesperrten Benutzerchipkarte.

Die Figur 1 zeigt ein System mit einer Zentrale 1, in welcher Parameter für eine Vielzahl von Chipkarten-Terminals in einem Speicherbereich 10 abgelegt sind. Die Zentrale 1 kann beispielsweise aus einem oder mehreren Rechnern bestehen, beispielsweise aus einem Server eines Finanzinstituts oder eines Dienstanbieters. Die Parameter im Speicherbereich 10 können beispielsweise Listen von gesperrten Benutzerchipkarten, Tarife, Saldi von elektronischen Bankkonten, Listen von durchgeführten Transaktionen, Benutzerprofile, kryptographische Schlüssel oder Zertifikate, usw. umfassen.

Eine Vielzahl von Online-Terminals 3 ist über ein Telekommunikationssystem 2 mit der Zentrale und eventuell auch untereinander verbunden. Das Telekommunikationsnetz 2 kann beispielsweise aus einem öffentlichen Netz (beispielsweise aus einem ISDN- oder Mobilfunk-Netz) bestehen, aus dem Internet, oder aus privaten Verbindungen, beispielsweise aus einem Privatnetz, beispielsweise ein LAN (Local Area Network) oder WAN (Wide Area Network). Je nach Anwendung können entweder tragbare Terminals 3 eingesetzt werden, die ihre Energie aus Batterien oder Solarzellen beziehen, oder stationäre Terminals, die aus dem Stromnetz oder aus Datenleitungen versorgt werden. Es können beispielsweise tragbare Mobilfunkgeräte 3 eingesetzt werden, beispielsweise Mobilfunktelefone gemäss GSM (Global System for Mobile Communication) oder gemäss UMTS (Universal Mobile Telecommunication System), oder tragbare Endgeräte mit einem Anschluss für ein Mobilfunkteil, beispielsweise in Form einer PC-Card. Als stationäre Terminals können beispielsweise Chipkarten-Terminals für Bankautomaten oder für Kassengeräte verwendet werden. Das System kann auch hybride Terminals umfassen, die nicht

ständig mit der Zentrale 1 verbunden sind, sondern die nur ab und zu (beispielsweise periodisch oder bei Bedarf) eine Verbindung herstellen.

Die Chipkarten-Terminals 3 umfassen einen Kartenleser und einen Terminalcomputer. Der Kartenleser in den die Benutzerchipkarte eingeschoben wird und der dann elektrisch kontaktiert wird, hat vor allem eine mechanische Funktion. Um den Kartenleser anzusteuern, die Benutzerschnittstelle zu verwalten und um die Verbindung zur Zentrale 1 und zu anderen Geräten herzustellen (beispielsweise zu einem Kassenautomaten) wird ein Terminalcomputer verwendet.

Die vorliegende Erfindung kann aber auch mit kontaktlosen Benutzerchipkarten verwendet werden, oder mit anderen RFID-Elementen (Radio Frequency Identication), beispielsweise in Uhren, Transpondern, in mit einer Funkschnittstelle ausgerüsteten Mobiltelefonen, in Palmtops, usw. Ebenso kann die vorliegende Erfindung mit Komponenten und Geräten eingesetzt werden, die eine Benutzeridentifizierung enthalten und die sich über eine Bluetooth Schnittstelle mit externen Terminals verbinden können, beispielsweise um Transaktionen durchzuführen.

Benutzerchipkarten 4 können in die Chipkarten-Terminals 3 eingeschoben werden, um Transaktionen durchzuführen. Je nach Anwendung und System kann die Chipkarte 4 beispielsweise aus einer Wertkarte bestehen, in welcher elektronische Geldeinheiten abgelegt sind, aus einer Telefonkarte, beispielsweise einer SIM (Subscriber Identification Module) oder WIM-Karte (WAP Identification Module) oder einer Telefonkarte für öffentliche Telefonzellen, aus einer Zutrittskarte für geschützte Systeme oder Gebäude usw. bestehen. Benutzerchipkarten werden in der Regel an alle autorisierten Benutzer der Terminals verteilt; mindestens gewisse Transaktionen mit dem Chipkartenterminal können nur mit einer gültigen Benutzerchipkarte durchgeführt werden.

Im Falle einer Wertkarte 4 können beispielsweise folgende Transaktionen mit dem Terminal 3 durchgeführt werden:

- Laden der Benutzerkarte mit elektronischen Geldeinheiten,
- Belasten des elektronischen Geldkontos in der Wertkarte 4 oder in der Zentrale 1,
- Prüfen des Geldkontos in der Wertkarte 4 oder in der Zentrale 1,
- Änderung des Zugriff-PINS oder des Geheimnisses,
- Prüfen der Identifizierung in der Karte 4, um damit Zugriff auf Systeme oder Dienstleistungen zu erlauben,
- Durchführung von kryptographischen Prozessen durch die Chipkarte 4 (z.B. digitale Signatur)
- usw.

Die Durchführung der Transaktionen ist abhängig von mehreren vergänglichen Parametern im Terminal 3, das heisst von Parametern die nur ab und zu aktualisiert werden müssen, beispielsweise täglich, wöchentlich, monatlich oder bei Bedarf. Je nach Art des Terminals können beispielsweise folgende vergängliche Parameter vorgesehen werden:

- Liste von gesperrten Benutzerchipkarten: Diese Liste enthält die Nummer oder Identifizierung von Karten, die nicht mehr gültig sind, beispielsweise weil das Gültigkeitsdatum abgelaufen ist, weil sie gestohlen oder missgebraucht wurden, usw.
- Tarife, vor allem bei Warenautomaten, in welchen die Benutzerchipkarte als Währungsmittel eingesetzt ist,

- Kryptographische Elemente, beispielsweise elektronische Schlüssel und/oder Zertifikate, Benutzer-Passwörter, usw.
- Bonitäten von Chipkartenbenutzern bei ihrem Finanzinstitut,
- Neue Software-Komponenten für den Terminal, beispielsweise als Applet oder CORBA-Komponenten,
- Parametertabellen für die im Terminal 3 durchgeführten Softwareanwendungen,
- Liste von den mit dem Terminal 3 durchgeführten Transaktionen,
- usw.

Je nach System können mindestens gewisse dieser Parameter auch im Speicherbereich 10 in der Zentrale 1 abgelegt werden, wie schon erwähnt.

Erfindungsgemäss werden mindestens gewisse dieser Parameter in mindestens gewisse Benutzerchipkarten 4 kopiert, die mit dem Terminal 3 verbunden werden und die ansonsten von den Benutzern für die Durchführung von normalen Transaktionen mit Terminals 3, 5 bestimmt sind. Vorzugsweise werden diese Parameter in einem gesicherten Speicherbereich 40, beispielsweise im EEPROM, welcher vom Benutzer der Chipkarte 4 nicht zugänglich ist, abgelegt. Vorzugsweise werden mindestens gewisse Parameter verschlüsselt, so dass nur autorisierte Chipkartenleser auf diese Parameter zugreifen können.

Die kopierten Parameter werden vorzugsweise mit einem Datum versehen, beispielsweise mit dem Datum der Übertragung in die Chipkarte 4 oder mit dem Herstellungsdatum der neuen Parameter. Werden die Parameter in eine Datei kopiert, ist es entweder möglich, die Datei mit

einem einzigen Datum zu versehen, oder jeden einzelnen Parameter. Befindet sich schon ein Parameter-Set in der Benutzerchipkarte 4, ist es möglich mit einem Synchronisierungsprogramm nur jene Parameter zu kopieren, die aktualisiert werden müssen. Das Datum kann entweder vom Terminal 3 oder von einem geeigneten Modul in der Benutzerchipkarte 4 gesetzt werden. Vorzugsweise wird ein elektronischer Zeitstempel verwendet, mit welchem die Echtheit des Datums geprüft werden kann. Ausserdem können mindestens gewisse Parameter mit einem Gültigkeitsdatum und/oder mit einer Gültigkeitsdauer versehen werden.

Es können auch Zeitelemente mit einer inkrementalen Uhr verwendet werden, die die Verwendung eines aufwendigeren Echtzeituhrelements erübrigen.

Die Figur 2 zeigt ein System mit einem Offline-Chipkarten-Terminal 5, mit welchem die Benutzerchipkarte 4 bei jeder Transaktion verbunden wird. Im Terminal 5 werden vergängliche Parameter (beispielsweise die oben angegebenen Parameter) in einem Speicherbereich 50 abgelegt. Erfindungsgemäss werden diese Parameter jedes Mal aktualisiert, wenn die Chipkarte 4 eines Benutzers für eine Transaktion in den Terminal 5 eingeschoben wird, indem der Terminal auf die im erwähnten Speicherbereich 40 gespeicherten Parameter zugreift und diese Parameter mit seinen eigenen vergleicht. Werden im Speicherbereich 40 Parameter abgelegt, die aktueller sind als die Parameter 50 im Terminal 5, oder die sich nicht im Terminal 5 befinden, kopiert ein geeignetes Modul im Terminal die neuen Parameter in den Speicherbereich 50, wobei ein Synchronisierungsmodul vorgesehen werden kann, um nur die neuesten Parameter zu kopieren.

Die vorliegende Erfindung eignet sich insbesondere dazu, Listen von gesperrten Benutzerchipkarten 6 in Offline-Terminals zu verteilen. Wenn die Zentrale 1 entscheidet eine Chipkarte zu sperren, kann sie durch das Telekommunikationssystem 2 die Identifizierung dieser Karte in alle Online-Terminals 3 kopieren, oder zumindest in allen Online-Terminals des geographischen Gebiets, in welchem die zu sperrende Chipkarte verwendet

wird. Die Karte 6 ist damit für die Verwendung mit Online-Terminals 3 gesperrt. Wird eine andere, gültige Benutzerchipkarte 4 in ein Online-Terminal 3 eingeschoben, kopiert der Terminal 3 die Identifizierung der gesperrten Karte im gesicherten Speicherbereich 40.

Sobald die Benutzerchipkarte 4 mit einem Offline-Terminal 5 verbunden wird, prüft ein geeignetes Modul im Terminal oder eventuell in der Benutzerchipkarte 4, ob die im Terminal abgelegte Liste von gesperrten Karten 50 aktualisiert werden muss. Ist dies der Fall, das heisst wenn die Identifizierung der gesperrten Karte 6 nicht in der Liste 50 enthalten ist, wird die Identifizierung dieser gesperrten Chipkarte 6 in den Terminal kopiert. Somit ist die Karte 6 für den Gebrauch mit diesem Terminal 5 gesperrt.

Der Fachmann wird verstehen, dass auch die gesperrte Karte 6 einen Speicherbereich 60 für Terminalparameter enthalten kann, und somit auch verwendet werden kann, um diese Parameter zu verteilen, wenn der Benutzer versucht, sie in verschiedenen Terminals zu verwenden.

Der Fachmann wird ausserdem verstehen, dass der gesicherte Speicherbereich 40 auch von den Offline-Terminals geschrieben werden kann. Auf diese Weise können auch Offline-Terminals 5 beispielsweise Listen von gesperrten Chipkarten 6 verteilen.

Dieses Verfahren kann auch eingesetzt werden, um Parameter und Dateien 50 aus Offline-Terminals über Benutzerchipkarten 4 und Online-Terminals 3 in die Zentrale zu übertragen. Es können über diesen Weg beispielsweise Listen der von vom Offline-Terminal gesperrten Karten, Listen der von mit dem Terminal 5 durchgeführten Transaktionen, oder elektronische Geldeinheiten von den Offline-Terminals in die Zentrale 1 übertragen werden. Auf diese Weise kann der Saldo der elektronischen Geldeinheiten in den Terminals 5 ausgeglichen werden und Geldeinheiten in die Zentrale 1 übertragen werden, ohne dass die Benutzer der Übertragungskarten 4 auf diese Einheiten zugreifen können.

Es sind Systeme bekannt, die Tausende von Chipkarten-Terminals 3, 5 und Millionen von Benutzerchipkarten 4 umfassen. In solchen Systemen kann die Liste der gesperrten Karten zu gross sein, um im begrenzten Speicherbereich einer Benutzerchipkarte gespeichert zu werden.

Um dieses Problem zu vermeiden, werden in einer bevorzugten Variante der Erfindung in einer Benutzerchipkarte 4 nur die Identifizierungen der zu sperrenden Chipkarten 6 gespeichert, die im selben begrenzten geographischen Gebiet verwendet werden (geographische Begrenzung der Liste). Vorzugsweise werden ausserdem nur die Identifizierungen der kürzlich (beispielsweise im letzten Jahr) gesperrten Karten kopiert. Auf diese Weise werden nur geographisch und zeitlich gezielte Informationen in Benutzerchipkarten kopiert.

In einer bevorzugten Variante der Erfindung werden unterschiedliche Sicherheitsanforderungen für beanspruchte Dienste und/oder für verwendete Terminals definiert. In diesem Fall werden mindestens gewisse Parameter nur in Terminals kopiert und/oder nur zur Sperrung von Diensten verwendet, die höhere Sicherheitsanforderungen verlangen. Es werden beispielsweise Listen von gesperrten Karten nur dann in Benutzerchipkarten kopiert, wenn diese Karten für hochgesicherte Dienste oder in hochgesicherten Offline-Terminals verwendet werden. Es können auch unterschiedliche Typen von Terminals und Anwendungen definiert werden, auf die mit denselben multifunktionellen Benutzerchipkarten zugegriffen werden kann, die aber unabhängig voneinander gesperrt oder aktualisiert werden können. Zu diesem Zweck können die benannten Parameter, die in Benutzerchipkarten kopiert werden, mit Terminal- und/oder Anwendungs-Angaben verknüpft werden.

Auf diese Weise werden nur für die Sicherheit wichtige Parameter in Benutzerchipkarten kopiert.

Ansprüche

1. Verfahren zur Aktualisierung von vergänglichen Parametern (50) in Offline-Chipkarten-Terminals (5), dadurch gekennzeichnet, dass die benannten vergänglichen Parameter mit den im benannten Offline-Chipkarten-Terminal (5) verwendeten Benutzerchipkarten (4) aktualisiert werden.

2. Verfahren gemäss dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass die benannten vergänglichen Parameter in die benannten Benutzerchipkarten (4) kopiert werden, wenn diese für eine Transaktion mit Online-Chipkarten-Terminals (3) verbunden sind.

3. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass mindestens gewisse benannte vergängliche Parameter in die benannten Benutzerchipkarten (4) kopiert werden, wenn diese mit Offline-Chipkarten-Terminals (5) verbunden sind.

4. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass mindestens gewisse vergängliche Parameter, die in der Benutzerchipkarte (4) eines Benutzers kopiert werden, andere Benutzerchipkarten (6) betreffen.

5. Verfahren gemäss dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass mindestens gewisse benannte vergängliche Parameter in einem vom Benutzer nicht zugänglichen Speicherbereich (40) der Benutzerchipkarte (4) abgelegt sind.

6. Verfahren gemäss dem Anspruch 3, dadurch gekennzeichnet, dass mindestens gewisse benannte vergängliche Parameter verschlüsselt sind.

7. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die benannten vergänglichen Parameter Tarife des benannten Offline-Chipkarten-Terminals (5) umfassen.

8. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die benannten vergänglichen Parameter Identifizierungen von gesperrten Benutzerchipkarten (6) umfassen.

9. Verfahren gemäss dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass die benannten Identifizierungen von gesperrten Benutzerchipkarten (6) nur in Benutzerchipkarten kopiert werden, die im selben geographischen Gebiet verwendet werden.

10. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die benannten vergänglichen Parameter mit einer Zeitangabe verknüpft sind.

11. Verfahren gemäss dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass die benannten vergänglichen Parameter mit einem Zeitstempel verknüpft sind.

12. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass Listen von durchgeführten Transaktionsparametern von den benannten Offline-Chipkarten-Terminals (5) in die benannten Benutzerchipkarten (4) kopiert werden.

13. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die benannten vergänglichen Parameter (40) elektronische Geldeinheiten umfassen, die über diesen Weg zwischen Offline-Chipkarten-Terminals (5) und Online-Chipkarten-Terminals (3) übertragen werden, ohne vom Benutzer der benannten Benutzerchipkarte verwendet werden zu können.

14. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass andere vergängliche Parameter über die benannten Benutzerchipkarten von den benannten Offline-Terminals in die benannten Online-Terminals kopiert werden.

15. Verfahren gemäss dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass die benannten anderen vergänglichen Parameter elektronische Geldeinheiten umfassen.

16. Benutzerchipkarte (4), die für die Durchführung von Transaktionen mit Offline-Chipkarten-Terminals (5) verbunden werden kann, dadurch gekennzeichnet, dass sie Parameter (40) umfasst, die zur Aktualisierung von vergänglichen Parametern in den benannten Chipkarten-Terminals bestimmt sind.

17. Benutzerchipkarte gemäss dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass mindestens gewisse benannten Parameter (40) andere Benutzerchipkarten (6) betreffen.

18. Benutzerchipkarte gemäss dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass die benannten Parameter (40) Listen von gesperrten Benutzerchipkarten (6) umfassen.

19. Benutzerchipkarte gemäss dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass die benannten Parameter nur Listen von gesperrten Benutzerchipkarten die im selben geographischen Gebiet verwendet wurden umfassen.

20. Benutzerchipkarte gemäss einem der Ansprüche 17 bis 19, dadurch gekennzeichnet, dass die benannten Parameter Listen von mit anderen Benutzerchipkarten durchgeführten Transaktionen umfassen.

21. Benutzerchipkarte gemäss einem der Ansprüche 16 bis 20, dadurch gekennzeichnet, dass mindestens gewisse benannten Parameter in einem vom Benutzer nicht zugänglichen Speicherbereich (40) der Benutzerchipkarte (4) abgelegt sind.

22. Benutzerchipkarte gemäss einem der Ansprüche 16 bis 21, dadurch gekennzeichnet, dass mindestens gewisse der benannten Parameter verschlüsselt sind.

23. Benutzerchipkarte gemäss einem der Ansprüche 16 bis 22, dadurch gekennzeichnet, dass die benannten Parameter Tarife umfassen.

24. Offline-Chipkarten-Terminal (5), der vergängliche Parameter verwendet, dadurch gekennzeichnet, dass er Datenverarbeitungsmittel umfasst, mit welchen die benannten vergänglichen Parameter aus mit dem Chipkarten-Terminal verbundenen Benutzerchipkarten (4) gelesen werden können.

25. Offline-Chipkarten-Terminal (5) gemäss dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass die benannten vergänglichen Parameter Listen von gesperrten Benutzerchipkarten (6) umfassen.

26. Chipkarten-Terminal (3), dadurch gekennzeichnet, dass er Datenverarbeitungsmittel umfasst, um Chipkartenarten (6), die gesperrt werden müssen, zu ermitteln, und um die Identifizierung dieser Benutzerchipkarten in andere Benutzerchipkarten (4) zu kopieren.

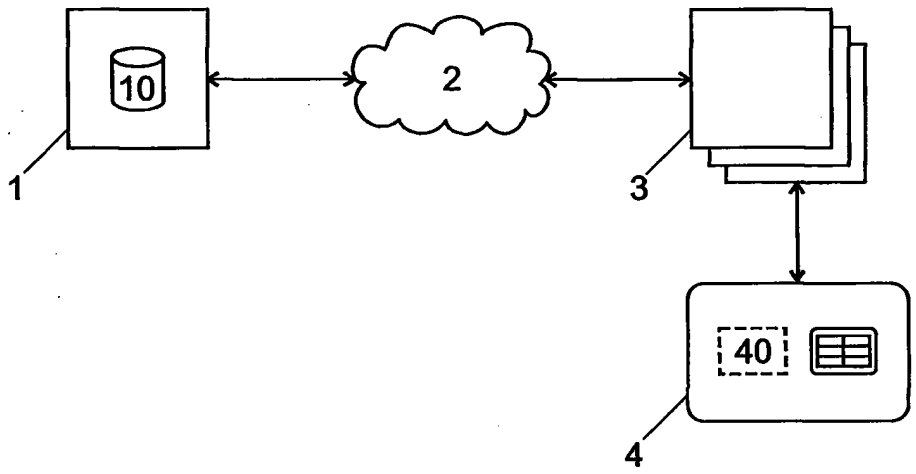


Fig. 1

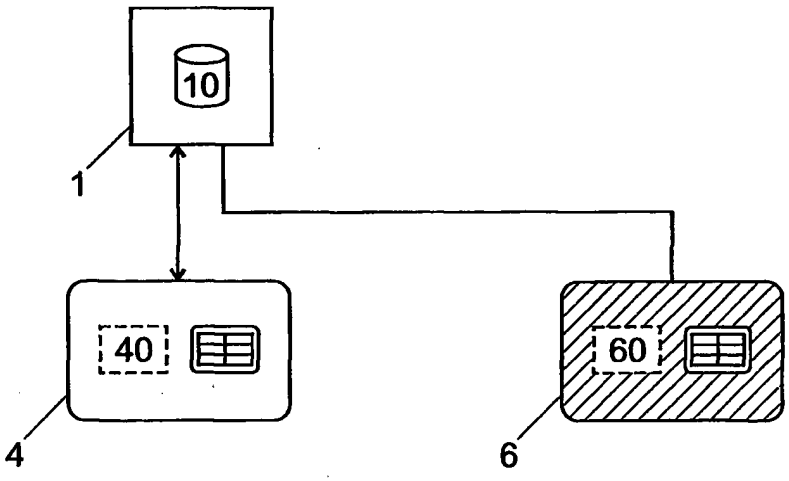


Fig. 2

INTERNATIONAL SEARCH REPORT

Inten Application No
PCT/CH 00/00149

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/08 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 97 36265 A (VRIEND GERRIT) 2 October 1997 (1997-10-02) the whole document	1-4,7,8, 13,14, 16-18, 23-26
X	US 5 276 312 A (MCCARTHY STEVEN R) 4 January 1994 (1994-01-04) column 4, line 64 -column 9, line 18 column 9, line 60 -column 12, line 56	1-3,6,7, 12,14, 16,22-24
X	GB 2 208 955 A (GEN ELECTRIC PLC) 19 April 1989 (1989-04-19) the whole document	1-3,7, 14,16, 23,24

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 December 2000	29/12/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Aupiais, B

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter al Application No
PCT/CH 00/00149

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 360 613 A (BALLY MFG CORP) 28 March 1990 (1990-03-28) column 4, line 14 -column 11, line 21	1,2,7,24
E	WO 00 21044 A (CAHORS APP ELEC ;ORENGO FRANCIS (FR)) 13 April 2000 (2000-04-13) page 1, line 5 -page 1, line 22 page 4, line 28 -page 7, line 26	1-3,6,7, 14,16, 22-24

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter al Application No
PCT/CH 00/00149

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9736265 A	02-10-1997	NL 1002733 C	30-09-1997
		CA 2249294 A	02-10-1997
		EP 0890158 A	13-01-1999
US 5276312 A	04-01-1994	AU 9153591 A	08-07-1992
		BR 9107145 A	19-04-1994
		MX 9102483 A,B	01-06-1992
		OA 9782 A	15-04-1994
		WO 9210806 A	25-06-1992
GB 2208955 A	19-04-1989	NONE	
EP 0360613 A	28-03-1990	US 5179517 A	12-01-1993
		AT 116754 T	15-01-1995
		AU 613484 B	01-08-1991
		AU 3450489 A	29-03-1990
		DE 68920391 D	16-02-1995
		DE 68920391 T	27-07-1995
WO 0021044 A	13-04-2000	FR 2784484 A	14-04-2000
		AU 5869599 A	26-04-2000

INTERNATIONALER RECHERCHENBERICHT

Intern[illegible]ales Aktenzeichen
PCT/CH 00/00149

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G07F7/08 G07F7/10

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G07F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	WO 97 36265 A (VRIEND GERRIT) 2. Oktober 1997 (1997-10-02) das ganze Dokument —	1-4,7,8, 13,14, 16-18, 23-26
X	US 5 276 312 A (MCCARTHY STEVEN R) 4. Januar 1994 (1994-01-04) Spalte 4, Zeile 64 -Spalte 9, Zeile 18 Spalte 9, Zeile 60 -Spalte 12, Zeile 56 —	1-3,6,7, 12,14, 16,22-24
X	GB 2 208 955 A (GEN ELECTRIC PLC) 19. April 1989 (1989-04-19) das ganze Dokument — -/—	1-3,7, 14,16, 23,24

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
20. Dezember 2000	29/12/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax (+31–70) 340–3016	Aupiais, B

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Inter ales Aktenzeichen
PCT/CH 00/00149

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 0 360 613 A (BALLY MFG CORP) 28. März 1990 (1990-03-28) Spalte 4, Zeile 14 -Spalte 11, Zeile 21	1,2,7,24
E	WO 00 21044 A (CAHORS APP ELEC ;ORENGO FRANCIS (FR)) 13. April 2000 (2000-04-13) Seite 1, Zeile 5 -Seite 1, Zeile 22 Seite 4, Zeile 28 -Seite 7, Zeile 26	1-3,6,7, 14,16, 22-24

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Intern les Aktenzeichen
PCT/CH 00/00149

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
WO 9736265	A	02-10-1997	NL	1002733 C	30-09-1997
			CA	2249294 A	02-10-1997
			EP	0890158 A	13-01-1999
US 5276312	A	04-01-1994	AU	9153591 A	08-07-1992
			BR	9107145 A	19-04-1994
			MX	9102483 A,B	01-06-1992
			OA	9782 A	15-04-1994
			WO	9210806 A	25-06-1992
GB 2208955	A	19-04-1989	KEINE		
EP 0360613	A	28-03-1990	US	5179517 A	12-01-1993
			AT	116754 T	15-01-1995
			AU	613484 B	01-08-1991
			AU	3450489 A	29-03-1990
			DE	68920391 D	16-02-1995
			DE	68920391 T	27-07-1995
WO 0021044	A	13-04-2000	FR	2784484 A	14-04-2000
			AU	5869599 A	26-04-2000